PCT/JP2004/014993

05.10.2004

日本国特許庁
JAPAN PATENT OFFICE

REC'D 18 NOV 2004

WIPO PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

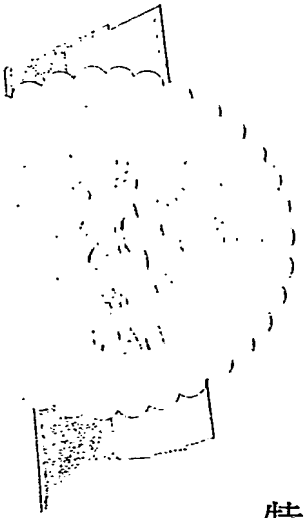
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年１０月１６日

出願番号
Application Number: 特願２００３－３５６０７２

[ST. 10/C]: [ＪＰ２００３－３５６０７２]

出願人
Applicant(s): 松下電器産業株式会社



PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

２００４年１１月 ５日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号 出証特２００４－３０９９９３４

【書類名】　特許願
【整理番号】　2022550333
【提出日】　平成15年10月16日
【あて先】　特許庁長官殿
【国際特許分類】　H04M　1/66
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　横田　薫
【発明者】
　【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内
　【氏名】　大森　基司
【特許出願人】
　【識別番号】　000005821
　【氏名又は名称】　松下電器産業株式会社
【代理人】
　【識別番号】　100097445
　【弁理士】
　【氏名又は名称】　岩橋　文雄
【選任した代理人】
　【識別番号】　100103355
　【弁理士】
　【氏名又は名称】　坂口　智康
【選任した代理人】
　【識別番号】　100109667
　【弁理士】
　【氏名又は名称】　内藤　浩樹
【手数料の表示】
　【予納台帳番号】　011305
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9809938

【書類名】特許請求の範囲
【請求項１】
携帯端末による記録担体アクセス方法であって、
　記録担体へのアクセスを許可する携帯端末の端末ＩＤリストからなるアクセス許可端末情報を前記記録担体の内部に登録する登録ステップと、
　前記携帯端末が前記記録担体に対して、アクセス要求及び前記携帯端末の端末ＩＤを送付するアクセス要求ステップと、
　前記アクセス要求ステップにおいて送付された前記端末ＩＤと、前記登録ステップにおいて登録したアクセス許可端末情報とを比較して、前記端末ＩＤが前記アクセス許可端末情報に含まれている場合には、前記携帯端末のアクセス要求を許可し、含まれていない場合には前記アクセス要求を拒否するアクセス許可判断ステップと
　を含むことを特徴とする記録担体アクセス方法。
【請求項２】
前記登録ステップは、
　登録用端末に１つあるいは２つ以上の端末ＩＤを入力する端末ＩＤ入力サブステップと、
　前記登録用端末が、前記端末ＩＤ入力ステップにおいて入力された１つあるいは２つ以上の端末ＩＤを含む登録要求データを前記記録担体に入力する登録要求データ入力サブステップと、
　前記記録担体が、前記登録要求データに含まれる１つあるいは２つ以上の端末を前記アクセス許可端末情報に追加するアクセス許可端末情報更新サブステップと
　を含むことを特徴とする請求項１に記載の記録担体アクセス方法。
【請求項３】
前記登録ステップは、携帯端末に認証コードを入力する認証コード入力ステップと、
　前記携帯端末が、前記認証コードと携帯端末自身の端末ＩＤとからなる登録要求データを前記記録担体に入力する登録要求データ入力ステップと、
　前記記録担体が、前記登録要求データに含まれる認証コードと記録担体内部に予め設定されている参照用認証コードとを比較して一致する場合に限り登録要求データに含まれる端末ＩＤを前記アクセス許可端末情報に追加するアクセス許可端末情報更新ステップと
　を含むことを特徴とする請求項１に記載の記録担体アクセス方法。
【請求項４】
前記登録ステップは、サーバーが前記携帯端末に、１つまたは２つ以上の携帯端末の端末ＩＤを含む登録指示データを送付する登録指示データ送付サブステップと、
　前記携帯端末が、前記登録指示データを前記記録担体に送付する登録指示データ転送サブステップと、
　前記記録担体が、前記登録データに含まれる１つまたは２つ以上の端末ＩＤを、内部に記憶するアクセス許可端末情報に追加するアクセス許可端末情報更新サブステップと
　を含むことを特徴とする請求項１に記載の記録担体アクセス方法。
【請求項５】
携帯端末による記録担体アクセス方法であって、
　記録担体へのアクセスを許可する携帯端末の端末ＩＤリストからなるアクセス許可端末情報をサーバーに登録する登録ステップと、
　前記携帯端末が前記記録担体に対して、アクセス要求及び前記携帯端末の端末ＩＤを送付するアクセス要求ステップと、
　前記アクセス要求を受けて、前記記録担体が前記携帯端末に対してアクセス許可端末情報を要求するアクセス許可端末情報要求ステップと、
　前記アクセス許可端末情報要求ステップを受けて、前記携帯端末が前記サーバーに登録されているアクセス許可端末情報を取得し、前記記録担体に送付するアクセス許可端末情報送付ステップと、
　前記アクセス許可端末情報送付ステップを受けて、前記アクセス要求ステップにおいて

送付された前記端末ＩＤと、前記アクセス許可端末情報送付ステップにおいて送付されたアクセス許可端末情報とを比較して、前記端末ＩＤが前記アクセス許可端末情報に含まれている場合には、前記携帯端末のアクセス要求を許可し、含まれていない場合には前記アクセス要求を拒否するアクセス許可判断ステップと
　を含むことを特徴とする記録担体アクセス方法。
【請求項６】
携帯端末からのアクセスを制御する機能を有する記録担体であって、
　外部からのアクセスを制限するアクセス制限領域と、外部からのアクセスを制限しない一般領域とからなるデータ記憶手段と、
　前記アクセス制限領域へのデータアクセスを許可する携帯端末の端末ＩＤのデータからなるアクセス許可端末情報を記憶するアクセス許可端末情報記憶手段と、
　外部からの登録要求に応じて、前記アクセス許可端末情報記憶手段に記憶するアクセス許可端末情報を更新するアクセス許可端末情報登録手段と、
　携帯端末から前記アクセス制限領域へのアクセス要求があった場合に、前記携帯端末の端末ＩＤと前記アクセス許可端末情報記憶手段に記憶するアクセス許可端末情報とを比較して、前記端末ＩＤが前記アクセス許可端末情報に含まれている場合には、前記携帯端末のアクセス要求を許可し、含まれていない場合には前記アクセス要求を拒否するアクセス制御手段と
　を備えることを特徴とする記録担体。
【請求項７】
前記アクセス許可端末情報登録手段は、
　外部からの登録要求データを受け付ける登録要求データ受付手段と、
　認証コードを記憶する認証コード記憶手段と、
　前記登録要求データに含まれる認証コードと前記認証コード記憶手段に記憶する認証コードとを比較する認証コード比較手段と、
　前記認証コード比較手段によって認証コードが一致すると判断された場合に限り、前記登録要求データに含まれる端末ＩＤを前記アクセス許可端末情報記憶手段に記憶するアクセス許可端末情報に追加するアクセス許可端末情報変更手段と
　を備えることを特徴とする請求項６に記載の記録担体。
【請求項８】
前記アクセス許可端末情報登録手段は、
　サーバーからネットワークを介して前記携帯端末に送付される登録要求データを受け付ける登録要求データ受付手段と、
　前記登録要求データに含まれる端末ＩＤを、前記アクセス許可端末情報記憶手段に記憶するアクセス許可端末情報に追加するアクセス許可端末情報更新手段と
　を備えることを特徴とする請求項６に記載の記録担体。
【請求項９】
携帯端末からのアクセスを制御する機能を有する記録担体であって、
　前記携帯端末からのアクセス要求及び前記携帯端末の端末ＩＤの送付を受けて、前記携帯端末に対してアクセス許可端末情報を要求するアクセス許可端末情報要求手段と、
　サーバーに記録されており、前記携帯端末を介して送付されるアクセス許可端末情報と前記端末ＩＤとを比較して、前記端末ＩＤが前記アクセス許可端末情報に含まれている場合には、前記携帯端末のアクセス要求を許可し、含まれていない場合には前記アクセス要求を拒否するアクセス制御手段と
　を備えることを特徴とする記録担体。
【請求項１０】
請求項７に記載の記録担体内のデータにアクセスする携帯端末であって、
　外部から認証コードの入力を受け付ける認証コード受付手段と、
　前記認証コードと携帯端末自身の端末ＩＤとを含む登録要求データを生成する登録要求データ生成手段と、

前記記録担体に前記登録要求データを前記記録担体に送付する登録要求データ送付手段と
を備えることを特徴とする携帯端末。
【請求項１１】
請求項９に記載の記録担体内のデータにアクセスする携帯端末であって、
前記記録担体へ、携帯端末自身の端末ＩＤを含むアクセス要求データを送付するアクセス要求データ送付手段と、
前記記録担体からのアクセス許可端末情報要求を受け付けるアクセス許可端末情報要求受付手段と、
アクセス許可端末情報を蓄積するサーバーからアクセス許可端末情報を受信するアクセス許可端末情報受信手段と、
受信したアクセス許可端末情報を前記記録担体に送付するアクセス許可端末情報送付手段と
を備えることを特徴とする請求項１０に記載の携帯端末。

【書類名】明細書
【発明の名称】記録担体アクセス方法、記録担体、携帯端末装置
【技術分野】
【０００１】
本発明は、ＳＩＭカードなどのＩＣカードやＳＤカード、メモリースティック、コンパクトフラッシュ（登録商標）などのメモリカードといった記録担体が装着可能な携帯端末機器及び記録担体に関するものであり、特に記録担体が盗難されたあるいは紛失した場合の対策として、携帯端末機器から記録担体内部のデータへのアクセスを制御する技術に関する。
【背景技術】
【０００２】
近年、携帯電話やＰＤＡ（Ｐｅｒｓｏｎａｌ　Ｄｉｇｉｔａｌ　Ａｓｓｉｓｔａｎｔ）などの携帯端末の高性能化、高機能化に伴い、ＳＩＭ（Ｓｕｂｓｃｒｉｂｅｒ　Ｉｄｅｎｔｉｔｙ　Ｍｏｄｕｌｅ）カードなどのＩＣカードや、ＳＤカード、メモリースティック、コンパクトフラッシュ（登録商標）などのメモリカードといった記録担体を装着するためのカードスロットを搭載した携帯端末が普及している。
【０００３】
それらの記録担体には、自分や知人の氏名、電話番号、メールアドレス、住所などの情報を含んだアドレス帳データや、カメラ付き携帯電話で撮影したデジタル写真データといった、プライベートな情報が記録されている。即ち、記録担体の保有者としては、他人に見られたくない個人情報に属するようなデータを記録担体に記録している。従って、万一その記録担体が盗難されたあるいは紛失した場合であっても、記録しているデータが他人には見られることがないような仕組みが必要になってくる。
【０００４】
上記のように記録担体の盗難／紛失に対する対策技術の第１の従来例として、特許文献１に開示されている方法がある。この方法では、記録担体は携帯電話機に装着されるＳＩＭカードを想定している。ＳＩＭカードは、携帯電話機の買い替えによる電話番号や登録データなどの移行をスムーズに行うために用いるもので、カードには、電話番号などのＩＤコードが登録、記録されているとともに、電話帳や着信履歴データが記録されている。買い替えなどにより携帯電話機を別の電話機に交換する場合には、現在の電話機に装着しているＳＩＭカードを新しい携帯電話機に差し替えるだけで、電話番号の移行と電話帳、着信履歴などの個人データの移行が行える。
【０００５】
本従来例では、ＳＩＭカードを盗んだ第３者がそのＳＩＭカードを自分の電話機に装着して電話をかけることによってその電話料金をＳＩＭカードの持ち主に負わせるような不正使用と電話帳や通話履歴などの個人データを覗き見る行為を防ぐことを目的としている。本従来例によると、ＳＩＭカードには前記のＩＤ情報、個人データの他に、固有の無効化コードが設定されている点に特徴がある。そして、万一、記録担体が盗難あるいは紛失にあった場合には、前記無効化コードを、前記ＳＩＭに装着された携帯電話機に電話をかけることによって送信する。無効化コードを受信した携帯電話機はそれをＳＩＭカードに転送し、受け取ったＳＩＭカードはその無効化コードが予めカード内に記憶しているものと一致するかを確認して一致する場合には、ＳＩＭカードのメモリのデータをロックして使用不能状態にする。これによって、他人のＳＩＭカードを用いて電話を掛ける不正使用や、カード内の個人情報覗き見を防止することが可能となる。
【０００６】
また、第２の従来例として、カード内のデータを他人の覗き見から守る一般的な方法であるパスワードによるデータロックの方法がある。この方法では、カード内には予めロックを解除するためのパスワードが設定されており、カード内のデータにアクセスするためには、パスワードを入力してロックを解除する必要がある。これにより、万一カードが他人の手に渡ったとしても、パスワードを知らないので他人によるカード内データの漏洩が

防止される。

【特許文献１】特開平１１－１７７６８２号公報

【発明の開示】

【発明が解決しようとする課題】

【０００７】

しかしながら、第１の従来例では、記録担体が外部から送信されるデータの受信が可能な携帯端末に装着されていることによって無効化コード送信によるカードロックが有効に働くことになる。即ち、盗まれた記録担体が、すぐに携帯端末から抜き取られ、オフラインで使用可能なカードデータ読み取り装置によって、カード内の電話帳データや通話履歴などの個人情報が全て抜き取られるような不正は阻止できない。また、近年携帯電話機にスロットが搭載されているＳＤカードやメモリースティックなどでは、電話帳のみならず、スケジュール帳やカメラ付き携帯電話で撮影したプライベート画像などの多くの個人のプライバシーに関わるデータが記憶されており、第１の従来例の方法をこれらのカードにも適用した場合には、前記オフラインによるカード読み取りによる個人情報流出の被害はより大きいものとなり深刻な問題となる。即ち、前記のようなカード内データの覗き見に対して、第１の従来例は、充分に防止できないという課題がある。

【０００８】

また、第２の従来例では、第１の従来例に関する上記のような課題は解決されるものの、正規カード保有者であっても記録担体内のデータにアクセスするたびに、パスワードを入力が要求されることになり、正規カード保有者の操作性を大きく損ねるという課題がある。

【０００９】

本発明は、前記従来の課題を解決するもので、第２の従来例のように正規カード保有者にとって操作の面で大きな負担をかけず、かつ、第１の従来例の課題としてあげたようなオフライン環境下でのカード内データの覗き見も防止することが可能な記録担体アクセス方法を提供することを目的とする。

【課題を解決するための手段】

【００１０】

前記従来の課題を解決するために、本発明の記録担体は、外部からのアクセスを制限するアクセス制限領域と、外部からのアクセスを制限しない一般領域とからなるデータ記憶手段と、前記アクセス制限領域へのデータアクセスを許可する携帯端末の端末ＩＤのデータからなるアクセス許可端末情報を記憶するアクセス許可端末情報記憶手段と、外部からの登録要求に応じて、前記アクセス許可端末情報記憶手段に記憶するアクセス許可端末情報を更新するアクセス許可端末情報登録手段と、携帯端末から前記アクセス制限領域へのアクセス要求があった場合に、前記携帯端末の端末ＩＤと前記アクセス許可端末情報記憶手段に記憶するアクセス許可端末情報とを比較して、前記端末ＩＤが前記アクセス許可端末情報に含まれている場合には、前記携帯端末のアクセス要求を許可し、含まれていない場合には前記アクセス要求を拒否するアクセス制御手段とを備える。

【００１１】

本構成によって、アクセス許可端末情報に含まれない携帯端末による記録担体へのアクセスを防止することができる。

【発明の効果】

【００１２】

本発明の記録担体によれば、正規カード保有者にとって操作の面で大きな負担をかけず、かつ、オフライン環境下でのカード内データの覗き見も防止することができる。また、本発明の記録担体アクセス方法によれば、ユーザーの操作負担を課さずに他人からのデータ覗き見に対する安全性を高めることができる。

【発明を実施するための最良の形態】

【００１３】

以下本発明の実施の形態について、図面を参照しながら説明する。

【００１４】
（実施の形態１）
図１は、本発明の実施の形態１において、携帯端末２が記録担体１内部のデータにアクセスする場合の構成図である。ここで、携帯端末２としては、携帯電話機などが、記録担体１としては、ＳＤカード、メモリースティックなどのメモリカードや、ＳＩＭカードなどのＩＣカードといったものが想定される。また、携帯端末２には記録担体１を装着するためのスロットがあり、記録担体１は前記スロットに装着されているものとする。
【００１５】
記録担体１は、携帯端末２とのデータやりとりを行う端末Ｉ／Ｆ１０と、記録担体１内部の動作を制御する制御部１１と、記録担体１の内部データにアクセス可能な機器の情報を記憶するアクセス可能機器情報記憶部１２と、データを記憶するデータ記憶部１３と、アクセス可能機器情報記憶部１２にアクセス可能機器情報の登録を行うアクセス可能機器情報登録部１５からなる。また、データ記憶部１３の内部には、アクセス可能機器情報記憶部１２に記憶するアクセス可能機器情報に基づいて、アクセスが制限されるアクセス制限領域１４が存在する。さらに、アクセス可能機器情報記憶部１２は外部からの直接アクセスができないようになっている。
【００１６】
携帯端末２は、記録担体１とのデータやりとりを行う記録担体Ｉ／Ｆ２０と、携帯端末を識別するための端末ＩＤを記憶する端末ＩＤ記憶部２１と、携帯端末２内部の動作を制御する制御部２２と、ユーザーによる携帯端末２外部からの入力を受信する外部入力Ｉ／Ｆ２３と、携帯端末２の内部データをユーザーに見える形にして表示する表示部２４からなる。
【００１７】
以下、携帯端末２が、記録担体１内のデータ記憶部１３にあるアクセス制限領域１４に記録されているデータにアクセスする場合の動作について説明する。
【００１８】
記録担体１内部のアクセス可能機器情報記憶部１２には、後で述べる方法によって既にアクセス可能機器情報が記憶されているものとする。
【００１９】
まず、携帯端末２に対してユーザーが記録担体１に記憶する所定データの表示要求を行う。具体的には、携帯端末２に搭載されている所定の入力ボタンを押下することによって行われる。その要求は外部入力Ｉ／Ｆ２３を介して制御部２２に伝達される。
【００２０】
前記要求を受けた制御部２２は、端末ＩＤ記憶部２１に記憶する端末ＩＤを読み出して、データアクセス要求とともに記録担体Ｉ／Ｆ２０を介して記録担体１に送信される。ここで端末ＩＤは各携帯端末を識別するための識別情報であり、例えば携帯電話の電話番号や、端末のシリアル番号などのようなものでよい。
【００２１】
前記データアクセス要求と端末ＩＤは記録担体１内部の端末Ｉ／Ｆ１０にて受信され、制御部１１に転送される。制御部１１は、アクセス可能機器情報記憶部１２に記憶されるアクセス可能機器情報を元に携帯端末２のデータアクセス要求を許可するかどうかを判断する。具体的には、前記アクセス可能機器情報は、記録担体１内部のアクセス制限領域１４にアクセス可能な携帯端末の端末ＩＤのリストからなり、制御部１１は、携帯端末２から送付されてきた端末ＩＤが前記リストの中に存在するかどうかをチェックしてアクセス要求を許可するかどうかを決定する。前記判断の結果、アクセス要求を許可する場合には、制御部１１は、データ記憶部１３内のアクセス制限領域１４の中から携帯端末２から要求されているデータを取得して、端末Ｉ／Ｆ１０を介して携帯端末２に送付する。アクセス要求を許可しない場合には、アクセス許可された端末でない旨を知らせる情報を端末Ｉ／Ｆ１０を介して携帯端末２に送付する。
【００２２】

記録担体１から前記データを受信した携帯端末２は、記録担体Ｉ／Ｆ２０を介して制御部２２に転送される。制御部２２は、受信したデータの内容を確認して、ユーザーが要求したデータである場合には、そのデータの内容を表示部２４に表示してユーザーに情報を提供する。一方、レスポンスのデータがアクセス許可された端末でない旨を知らせる内容である場合には、表示部２４にこの携帯端末が要求されたデータにアクセスすることを許可されていないことを示すメッセージを表示させる。

【００２３】

次に、アクセス可能機器情報記憶部１２にアクセス可能機器情報を記憶／更新する方法について説明する。

【００２４】

図２は、本発明の実施の形態１においてアクセス可能機器情報記憶部１２にアクセス可能機器情報を記憶／更新するための第１の方法に関する機器構成を示したものである。図２において、記録担体１は、図１に示す記録担体１と同一のものである。アクセス可能機器情報登録器３は、記録担体１内部のアクセス可能機器情報記憶部１２にアクセス可能機器情報を登録するための専用機器であり、機器外部から端末ＩＤの入力を受け付けて書き込み許可データ生成部３１に転送する外部入力Ｉ／Ｆ３０と、外部入力Ｉ／Ｆ３０から転送された端末ＩＤデータを元に、アクセス可能機器情報登録指示データを作成して記録担体Ｉ／Ｆ３２に転送する書き込み許可データ生成部３１と、前記アクセス可能機器情報登録指示データを記録担体１に転送する記録担体Ｉ／Ｆ３２からなる。本実施の形態において、アクセス可能機器情報の登録は、登録処理が認められた専用の機器（即ち、アクセス可能機器情報登録器３のような専用機器）以外では行うことができないものとする。また、アクセス可能機器情報登録器３は記録担体１を装着するためのスロットを有しており、記録担体１はこのスロットに装着された状態で以下の動作が行われるものとする。

【００２５】

以下、アクセス可能機器情報登録器３を用いて記録担体１にアクセス可能機器情報を記憶／更新する際の動作について説明する。

【００２６】

まず、記録担体１にアクセス可能機器を登録する処理なのか、あるいは、既に登録されているアクセス可能機器の登録削除を行う処理なのかを示す登録／登録削除指示データと、登録あるいは登録削除を行う対象となる携帯端末の端末ＩＤがアクセス可能機器情報登録器３に外部から入力される。このとき、登録あるいは登録削除する端末ＩＤは１つである必要はなく、１度の処理で複数の端末ＩＤを入力してもよい。外部から入力される登録／登録削除指示データと端末ＩＤは外部入力Ｉ／Ｆ３０で受け付けられ、外部入力Ｉ／Ｆ３０は、入力された端末ＩＤを書き込み許可データ生成部３１に転送する。次に、書き込み許可データ生成部３１は、入力された登録／登録削除指示データと端末ＩＤをもとに記録担体処理データを作成する。記録担体処理データの具体内容としては、アクセス可能機器情報記憶部１２への端末ＩＤ登録／登録削除を指示するためのコマンドコードと、そのコマンドコードの実行によって登録／登録削除を行う端末ＩＤの個数と、登録／登録削除を行う端末ＩＤのリストを結合したデータ列からなる。この記録担体処理データは記録担体Ｉ／Ｆ３２を介して記録担体１に送付される。

【００２７】

前記記録担体処理データは、記録担体１内部の端末Ｉ／Ｆ１０で受け付けられて、アクセス可能機器情報登録部１５に転送される。アクセス可能機器情報登録部１５は、入力された記録担体処理データを解釈して、アクセス可能機器情報記憶部１２に記憶しているアクセス可能機器情報の更新を行う。具体的には、アクセス可能機器の登録を行う指示のデータを受け取った場合には、データが指定する端末ＩＤをアクセス可能機器情報に追加する。このとき、指定する端末ＩＤが既にアクセス可能機器情報として登録済みの場合には、アクセス可能機器情報登録器３にその旨のエラーメッセージを返す。また、アクセス可能機器の削除を行う指示のデータを受け取った場合には、データが指定する端末ＩＤをアクセス可能機器情報から削除する。このとき、指定する端末ＩＤがアクセス可能機器情報

に登録されていない場合には、アクセス可能機器情報登録器３にその旨のエラーメッセージを返す。上記の一連の処理によってアクセス可能機器情報記憶部１２に記憶するアクセス可能機器情報が更新される。

【００２８】

このとき、アクセス可能機器情報の不正規な登録／削除処理が記録担体１に対して行われるのを避けるために、以下のような処理を追加してもよい。即ち、アクセス可能機器情報登録器３は、公開鍵暗号方式を用いたデジタル署名方式の署名鍵を秘密に保持し、書き込み許可データ生成部３１は生成した記録担体処理データに前記署名鍵を用いてデジタル署名を施した上で記録担体１に送付する。一方、記録担体１は、前記署名を検証するための検証鍵を保持しており、アクセス可能機器情報登録部１５は、前記記録担体処理データの指示に従った処理を行う前に、前記検証鍵を用いて記録担体処理データに施されたデジタル署名の正当性を検証する。このとき、署名の正当性が確認された場合にのみ、その記録担体処理データが正規のアクセス可能機器情報登録器から発行されたデータであると判断して登録／登録処理を継続する。一方、デジタル署名の正当性が確認できなかった場合には、その記録担体処理データを不正なものとして以降の処理を行わないようにする。

【００２９】

また、過去の登録／登録削除処理に使用された記録担体処理データを保存しておいて、それを再び記録担体に送付して登録／登録削除処理を実行させるような不正対策、及び、不正規のアクセス可能機器情報登録器による登録／登録削除処理を防止する手段として以下のような処理を追加してもよい。即ち、前記の追加処理と同様に、アクセス可能機器情報登録器３には署名鍵、記録担体１にはそれに対応する検証鍵を保持しておく。そして、前記の登録／登録削除処理を行う際には、次のステップからなるチャレンジレスポンス認証を行う。

【００３０】

１．記録担体１が、乱数を発生してアクセス可能機器情報登録器３に送付する

２．アクセス可能機器情報登録器３が、前記乱数に対して署名鍵を用いて署名を施して記録担体１に返送する

３．記録担体１が、検証鍵を用いて前記署名を検証する

３．において、署名が正当であると確認できたときに限り、登録／登録削除処理を継続し、正当であると確認できなかった場合には登録／登録削除処理を行わない。これによって、正規のアクセス可能機器情報登録器のみが登録／登録削除処理を行え、かつ、同時に不正規登録器が過去の記録担体処理データを再送付して登録／登録削除処理を行うことを防止している。

【００３１】

次に、アクセス可能機器情報を登録する第２の方法について説明する。図３は、本発明の実施の形態１におけるアクセス可能機器情報記憶部１２にアクセス可能機器情報を登録する第２の方法に関する機器構成を示したものである。図３において、記録担体１及び携帯端末２は、図１に示す記録担体１及び携帯端末２と同一のものである。以下は、記録担体１に対して携帯端末２をアクセス可能機器として登録あるいは登録削除する場合の動作について説明している。また、以下の動作は記録担体１が携帯端末２に装着されている状態で行われるものとする。

【００３２】

記録担体１には、予め所定のパスワードが設定されアクセス可能機器情報記憶部１２に記憶されているものとする。これは、例えば、記録担体製造または出荷時にカード固有のパスワードが設定されており、パッケージの箱を開けることで初めて見ることのできる個所にパスワード情報を印刷するなどして、記録担体の購入者のみに知らせるようにすれば良い。

【００３３】

まず、携帯端末２に対して記録担体１に設定されているパスワードと、登録／登録削除指示データとが外部から入力される。入力された前記データは、携帯端末２内部の外部入

力Ｉ／Ｆ２３で受け付けて制御部２２に転送される。制御部２２は、前記入力データに、端末ＩＤ記憶部２１が記憶する携帯端末２の端末ＩＤを付加した上で、記録担体Ｉ／Ｆ２０を介して記録担体１に送付する。即ち、パスワードと、登録／登録削除指示データと、携帯端末２の端末ＩＤが記録担体１に送付される。このデータは、記録担体１内部の端末Ｉ／Ｆ１０で受け付けて、アクセス可能機器情報登録部１５に入力される。

【００３４】

次に、アクセス可能機器情報登録部１５は、前記入力データに含まれるパスワードがアクセス可能機器情報記憶部１２に記憶している記録担体１のパスワードと一致するかを確認し、一致する場合には、以下の処理を行う。一致しない場合には、処理を行わない。前記パスワード確認の後、入力データに含まれる登録／登録削除指示データとその処理対象となる端末ＩＤに従って、アクセス可能機器情報記憶部１２に記憶するアクセス可能機器情報を更新する。このとき、アクセス可能機器情報を登録する第１の方法の説明でも述べたように、既に登録済みの端末ＩＤの登録指示である場合、あるいは、登録されていない端末ＩＤの登録削除指示である場合には、その旨のエラーメッセージを携帯端末２に返す。また、携帯端末２から送られてくるパスワード、登録／登録削除指示データ、端末ＩＤが記録担体に送付される過程において改ざんされるのを防止するために、前記第１の方法の場合と同様にして、前記データに対して携帯端末２内部の制御部２２でデジタル署名を施し、記録担体１内部のアクセス可能機器情報登録部１５で前記デジタル署名の正当性を検証するようにしてもよい。

【００３５】

さらに、アクセス可能機器情報を登録する第３の方法について説明する。第３の方法では、記録担体へのアクセス可能機器情報登録／登録削除依頼をアクセス可能機器情報配信サーバー４に対して行い、前記サーバーは、その受け付けた依頼内容に基づいて記録担体１に対してアクセス可能機器情報の更新処理を行う。このとき、サーバーと記録担体は携帯端末２を介してネットワーク経由で前記更新処理を行う。図４は、本発明の実施の形態１におけるアクセス可能機器情報記憶部１２にアクセス可能機器情報を登録する第３の方法に関する機器構成を示したものである。

【００３６】

図４において、携帯端末２は、図１に示す携帯端末２において、ネットワーク経由でデータの送受信を行う通信Ｉ／Ｆ２５が追加された構成となっている。記録担体１は、図１に示す記録担体１において、各記録担体に固有のＩＤ番号（カードＩＤ）を記憶するカードＩＤ記憶部１６が追加された構成となっている。また、アクセス可能機器情報配信サーバー４は、ユーザーからのアクセス可能機器情報登録／登録削除依頼を受けてネットワーク経由で記録担体に記憶するアクセス可能機器情報の更新を行うものであり、外部からの入力データを受け付けて書き込み許可データ生成部４１に転送する外部入力Ｉ／Ｆ４０と、前記入力データをもとに記録担体１に送付するための書き込み許可データを生成してデータ送信部４２に転送する書き込み許可データ生成部４１と、前記書き込み許可データを携帯端末２にネットワーク経由で送付するデータ送信部４２からなる。以下、アクセス可能機器情報登録／登録削除を行う際の動作について説明する。なお、以下の動作は記録担体１が携帯端末２に装着された状態で行われるものとする。

【００３７】

まず、アクセス可能機器情報配信サーバー４に、依頼データが入力される。依頼データは具体的には、アクセス可能機器情報の登録あるいは登録削除のどちらを行うのかを示す登録／登録削除指示データと、登録／登録削除を行う端末ＩＤと、登録／登録削除を行う対象となる記録担体のカードＩＤと、本依頼データに基づく登録／登録削除を指示する書き込み許可データの送付先携帯端末を示す送付先データからなる。

【００３８】

送付先データの具体的な内容としては、携帯端末２が携帯電話などの場合には電話番号、メール受信機能のある端末の場合にはメールアドレス、ＩＰ接続可能な端末の場合にはＩＰアドレスなどが考えられる。

【００３９】
入力された前記依頼データは、外部入力Ｉ／Ｆ４０で受け付けて書き込み許可データ生成部４１に転送される。前記入力を受けて、書き込み許可データ生成部４１は、前記依頼データを元に書き込み許可データを生成してデータ送信部４２に転送する。書き込み許可データは、具体的には、書き込み許可データの送信先を示す送付先データと、本書き込み許可データに含まれる端末ＩＤの登録／登録削除処理をどの記録担体に対して指示しているのかを示すカードＩＤと、登録／登録削除のどちらを指示するのかを示す登録／登録削除指示データと、登録／登録削除を行う端末ＩＤの情報を含んでいる。データ送信部４２は、前記書き込み許可データに含まれる送付先データが指定する携帯端末２に書き込み許可データを送信する。
【００４０】
前記書き込み許可データは携帯端末２内部の通信Ｉ／Ｆ２５にて受信し、制御部２２に転送する。さらに制御部２２は、前記書き込みデータを記録担体Ｉ／Ｆ２０を介して記録担体１に送付する。
【００４１】
記録担体１に送付された書き込み許可データは、端末Ｉ／Ｆ１０にて受信し、アクセス可能機器情報登録部１５に転送する。アクセス可能機器情報登録部１５は、まず入力された書き込み許可データに含まれるカードＩＤとカードＩＤ記憶部１６に記憶される記録担体１のカードＩＤとが一致することを確認する。もしも一致しない場合には、本書き込み許可データが記録担体１に対して発行されたものではない旨のエラーメッセージを携帯端末２に返して処理を終了する。一致する場合は、以下の処理を続行する。次に、書き込み許可データに含まれる、登録／登録削除指示データと端末ＩＤに従って、アクセス可能機器情報記憶部１２に記憶するアクセス可能機器情報を更新する。このとき、アクセス可能機器情報を登録する第１、第２の方法の説明でも述べたように、既に登録済みの端末ＩＤの登録指示である場合あるいは、登録されていない端末ＩＤの登録削除指示である場合には、その旨のエラーメッセージを携帯端末２に返すようにしてもよい。また、書き込み許可データが、アクセス可能機器情報配信サーバー４から携帯端末２経由で記録担体１に送付される過程における改ざん、及び、偽造された書き込み許可データが記録担体１に送付され処理されるのを防止するために、前記第１、第２の方法の場合と同様にして、アクセス可能機器情報配信サーバー４はデジタル署名生成用の署名鍵を秘密に保持して、内部の書き込み許可データ生成部４１において生成した書き込み許可データに対してデジタル署名を施して送付するようにしてもよい。このとき記録担体１内部では前記デジタル署名を検証するための検証鍵を保持して、アクセス可能機器情報登録部１５で前記デジタル署名の正当性を検証する。
【００４２】
また、過去の登録／登録削除処理に使用された記録担体処理データを保存しておいて、それを再び記録担体１に送付して登録／登録削除処理を実行させるような不正対策として以下のような処理を追加してもよい。即ち、前記の追加処理と同様に、アクセス可能機器情報配信サーバー４には署名鍵、記録担体１にはそれに対応する検証鍵を保持しておく。そして、前記の登録／登録削除処理を行う際には、次のステップからなるチャレンジレスポンス認証を行う。
【００４３】
１．記録担体１が、乱数を発生してアクセス可能機器情報配信サーバー４に送付する
２．アクセス可能機器情報配信サーバー４が、前記乱数に対して署名鍵を用いて署名を施して記録担体１に返送する
３．記録担体１が、検証鍵を用いて前記署名を検証する
３．において、署名が正当であると確認できたときに限り、登録／登録削除処理を継続し、正当であると確認できなかった場合には登録／登録削除処理を行わない。これによって、正規のアクセス可能機器情報配信サーバーのみが登録／登録削除処理を行えるので、不正規のアクセス可能機器情報配信サーバーあるいは携帯端末が過去の記録担体処理デー

タを再送付して登録／登録削除処理を行うことを防止できる。

【００４４】

かかる構成によれば、記録担体にアクセス可能な端末の端末ＩＤを記録担体内部に保持することにより、携帯端末がネットワークに接続していないオフラインの状態であっても、アクセス可能な端末として登録されていない携帯端末によるアクセスを拒絶する。これによって、第１の従来例では可能であったオフラインの状態でのカードの不正使用を阻止することができ、かつ、第２の従来例のようにカードにアクセスするたびにパスワードの入力を要求するというようなユーザー負担をなくすことができる。

【００４５】

（実施の形態２）

実施の形態１では、記録担体へのアクセス許可／拒絶を判断するためのアクセス可能機器情報をその記録担体自身の内部に記録していた。実施の形態２は、アクセス可能機器情報をネットワーク上に存在するアクセス可能機器情報を蓄積配信するためのサーバーに記憶するところに特徴がある。携帯端末からのアクセス要求が来ると、その都度、記録担体は前記サーバーからアクセス可能機器情報を取得してアクセス許可／拒絶の判断を行う。以下、その詳細について説明する。

【００４６】

図５は、本発明の実施の形態２において、携帯端末６が記録担体５内部のデータにアクセスする場合の構成図である。このとき、記録担体５は、アクセス可能機器情報管理サーバー７から送られるアクセス可能機器情報に基づいて、携帯端末６によるデータアクセスを許可するかどうかを判断する。

【００４７】

記録担体５は、携帯端末６とのデータやりとりを行う端末Ｉ／Ｆ５０と、記録担体５内部の動作を制御する制御部５１と、アクセス可能機器情報管理サーバー７から送られてくるアクセス可能機器情報が改ざんされていないかをチェックするアクセス可能機器情報改ざん検査部５２と、データを記憶するデータ記憶部５３と、記録担体５ごとに固有のＩＤ番号であるカードＩＤを記憶するカードＩＤ記憶部５５からなる。また、データ記憶部５３の内部には、アクセス可能機器情報管理サーバー７から送られてくるアクセス可能機器情報に基づいて、アクセスが制限されるアクセス制限領域５４が存在する。

【００４８】

携帯端末６は、記録担体５とのデータやりとりを行う記録担体Ｉ／Ｆ６０と、携帯端末６を識別するための端末ＩＤを記憶する端末ＩＤ記憶部６１と、携帯端末６内部の動作を制御する制御部６２と、ユーザーによる携帯端末６外部からの入力を受信する外部入力Ｉ／Ｆ６３と、携帯端末６の内部データをユーザーに見える形にして表示する表示部６４と、ネットワーク経由でデータの送受信を行う通信Ｉ／Ｆ６５からなる。

【００４９】

アクセス可能機器情報管理サーバー７は、各記録担体のアクセス可能機器情報を記憶するアクセス可能機器情報記憶部７０と、アクセス可能機器情報記憶部７０に記憶するアクセス可能機器情報の更新を行うアクセス可能機器情報登録部７１からなる。

【００５０】

以下、携帯端末６が、記録担体５内のデータ記憶部５３にあるアクセス制限領域５４に記録されているデータにアクセスする場合の動作について説明する。なお、携帯端末６には記録担体５を装着するためのスロットがあり、以下の動作では記録担体５が携帯端末６のスロットに装着された状態で行われるものとする。

【００５１】

アクセス可能機器情報管理サーバー７には、予めデジタル署名用の署名鍵が秘密に保持されているものとする。また、前記デジタル署名を検証するための検証鍵が記録担体５内部のアクセス可能機器情報改ざん検査部５２に記憶されているものとする。さらに、アクセス可能機器情報管理サーバー７内部のアクセス可能機器情報記憶部７０には、後で述べる方法によって記録担体ごとのアクセス可能機器情報が記憶されているものとする。まず

、携帯端末６に対してユーザーが記録担体５に記憶する所定データの表示要求を行う。具体的には、携帯端末６に搭載されている所定の入力ボタンを押下することによって行われる。その要求は外部入力Ｉ／Ｆ６３を介して制御部６２に伝達される。

【００５２】

前記要求を受けた制御部６２は、端末ＩＤ記憶部６１に記憶する端末ＩＤを読み出して、データアクセス要求とともに記録担体Ｉ／Ｆ６０を介して記録担体５に送信される。ここで端末ＩＤは各携帯端末を識別するための情報であり、例えば携帯電話の電話番号や、端末のシリアル番号などのようなものである。

【００５３】

前記データアクセス要求と端末ＩＤは記録担体５内部の端末Ｉ／Ｆ５０で受信され、制御部５１に転送される。上記データを受け取った制御部５１は、カードＩＤ記憶部５５に記憶する記憶担体５のカードＩＤを読み出した後、携帯端末６を経由してアクセス可能機器情報管理サーバー７に対して前記カードＩＤを送付し、送付したカードＩＤに対応するアクセス可能機器情報の送付を要求する。前記要求を受けたサーバー７は、アクセス可能機器情報記憶部７０において、受け取ったカードＩＤに対応するアクセス可能機器情報を検索して取り出し、さらに取り出したアクセス可能機器情報に対して署名鍵を用いてデジタル署名を施したものを携帯端末６経由で記録担体５に送付する。

【００５４】

前記アクセス可能機器情報を受け取った制御部５１は、アクセス可能機器情報改ざん検査部５２において、検証鍵を用いてアクセス可能機器情報に施されたデジタル署名の正当性を検証し、正当と判断された場合に限り以下の処理を続行する。正当でないと判断された場合には、その旨のエラーメッセージを携帯端末６に返して処理を中止する。また、前記アクセス可能機器情報の送付要求後、一定の時間が経過してもアクセス可能機器情報が受信されない場合にも、その旨のエラーメッセージを返して処理を中止する。

【００５５】

次に、正当性の検証できたアクセス可能機器情報を元に携帯端末６のデータアクセス要求を許可するかどうかを判断する。具体的には、前記アクセス可能機器情報は、記録担体５内部のアクセス制限領域５４にアクセス可能な携帯端末の端末ＩＤのリストからなり、制御部５１は、携帯端末６から送付されてきた端末ＩＤが前記リストの中に存在するかどうかをチェックしてアクセス要求を許可するかどうかを決定する。前記判断の結果、アクセス要求を許可する場合には、制御部５１は、データ記憶部５３内のアクセス制限領域５４の中から携帯端末６から要求されているデータを取得して、端末Ｉ／Ｆ５０を介して携帯端末６に送付する。アクセス要求を許可しない場合には、アクセス許可された端末でない旨を知らせるデータを端末Ｉ／Ｆ５０を介して携帯端末６に送付する。

【００５６】

記録担体５から前記データを受信した携帯端末６は、記録担体Ｉ／Ｆ６０を介して制御部６２に転送される。制御部６２は、受信したデータの内容を確認して、ユーザーが要求したデータである場合には、そのデータの内容を表示部６４に表示してユーザーに情報を提供する。一方、受信したデータがアクセス許可された端末でない旨を知らせるものである場合には、表示部６４にこの携帯端末が要求されたデータにアクセスすることを許可されていないことを示すメッセージを表示させる。

【００５７】

次に、アクセス可能機器情報管理サーバー７内部のアクセス可能機器情報記憶部７０にアクセス可能機器情報を登録／更新する方法について説明する。

【００５８】

図６は、本発明の実施の形態2におけるアクセス可能機器情報管理サーバー７内部のアクセス可能機器情報記憶部７０にアクセス可能機器情報を登録／更新する方法に関する機器構成を示したものである。図６において、アクセス可能機器情報管理サーバー７は、図５に示すものと同一のものである。ユーザー端末８は、ネットワーク経由でアクセス可能機器情報管理サーバー７にアクセスしてアクセス可能機器情報の登録／更新を行うための

端末であるが、専用端末である必要はなく、例えばネットワーク接続可能なＰＣや、携帯電話、ＰＤＡのようなものであってもよい。以下ユーザー端末８を用いてアクセス可能機器情報の登録／更新を行う際の動作を説明する。

【００５９】

ユーザーは予めアクセス可能機器情報管理サーバー７にユーザー名とユーザーパスワードを登録しておく。

【００６０】

まずユーザー端末８がアクセス機能機器情報管理サーバー７に接続する際に、前記ユーザー名とユーザーパスワードがユーザー端末８に入力される。前記入力データは、外部入力Ｉ／Ｆ８０、制御部８１、通信Ｉ／Ｆ８２を介してアクセス可能機器情報管理サーバー７に送信され、アクセス可能機器情報管理サーバー７は、受け取ったユーザー名とユーザーパスワードが登録されているものと一致することを確認し、一致するときに限り以下の処理を続行する。一致しない場合には処理を中止する。

【００６１】

次に、ユーザー端末８に、アクセス可能機器情報を登録／登録削除したい記録担体のカードＩＤ、アクセス可能機器情報の登録あるいは登録削除を指示するための登録／登録削除指示データ、及び登録／登録削除したい携帯端末の端末ＩＤからなる依頼データを入力する。入力された依頼データは外部入力Ｉ／Ｆ８０で受け付けて、制御部８１、通信Ｉ／Ｆ８２を介してアクセス可能機器情報管理サーバー７に送信される。

【００６２】

アクセス可能機器情報管理サーバー７で受信した前記依頼データは、アクセス可能機器情報登録部７１にて処理される。具体的には、依頼データに含まれるカードＩＤに対応するアクセス可能機器情報をアクセス可能機器情報記憶部７０に記憶するデータから検索して取り出し、登録／登録削除指示データの指示に従って、指定される端末ＩＤの登録あるいは登録削除を行い、前記取り出したアクセス可能機器情報を更新して再びアクセス可能機器情報記憶部７０に記憶する。このとき、依頼データに基づく指示が既にアクセス可能機器情報に登録されている端末ＩＤの登録処理である場合、あるいは、アクセス可能機器情報に登録されていない端末ＩＤの登録削除処理である場合、もしくは、ユーザーが所有していないはずのカードＩＤに対する登録／登録削除処理である場合には、その旨を示すエラーメッセージをユーザー端末８に返す。

【００６３】

かかる構成によれば、アクセス可能機器情報をサーバーに記憶／管理して、携帯端末が記録担体にアクセスする際には、記録担体はサーバーからアクセス可能機器情報の取得を要求して、取得したアクセス可能機器情報に基づいて携帯端末のアクセスを制御する。また、アクセス可能機器情報の取得に失敗した場合には携帯端末のアクセスを拒絶する。これにより、携帯端末がネットワークに接続していないオフラインの状態では、記録担体へのアクセスができないので、第１の従来例では可能であったオフラインの状態でのカードの不正使用を阻止することができ、かつ、第２の従来例のようにカードにアクセスするたびにパスワードの入力を要求するというようなユーザー負担をなくすことができた。

【００６４】

さらに、本実施形態では、記録担体とともにアクセス可能機器情報に登録されている携帯端末までもが盗まれるあるいは紛失した場合であっても、ユーザーはユーザー端末を用いてアクセス可能機器情報から前記携帯端末の端末ＩＤを登録削除すれば記録担体の不正使用を阻止できるというメリットもある。

【産業上の利用可能性】

【００６５】

本発明にかかる記録担体は、記録担体の盗難／紛失時の不正利用に対する安全性を高めつつユーザー側の処理負荷は増加させないという効果を有するので、例えば個人情報や金銭データなどを記憶したＩＣカードなどに適用可能である。また、前記の例に限らず、不正使用されたくない重要なデータを記録するメモリカードであれば何でも適用が可能であ

る。

【図面の簡単な説明】

【００６６】

【図１】本発明の実施の形態１に係る記録担体アクセス時の記録担体１及び携帯端末２の構成を示すブロック図

【図２】本発明の実施の形態１に係るアクセス可能機器情報登録時の第１の方法における記録担体１及びアクセス可能機器情報登録器３の構成を示すブロック図

【図３】本発明の実施の形態１に係るアクセス可能機器情報登録時の第２の方法における記録担体１及び携帯端末２の構成を示すブロック図

【図４】本発明の実施の形態１に係るアクセス可能機器情報登録時の第３の方法における記録担体１、携帯端末２、及びアクセス可能機器情報配信サーバー４の構成を示すブロック図

【図５】本発明の実施の形態２に係る記録担体アクセス時の記録担体５、携帯端末６、及びアクセス可能機器情報管理サーバー７の構成を示すブロック図

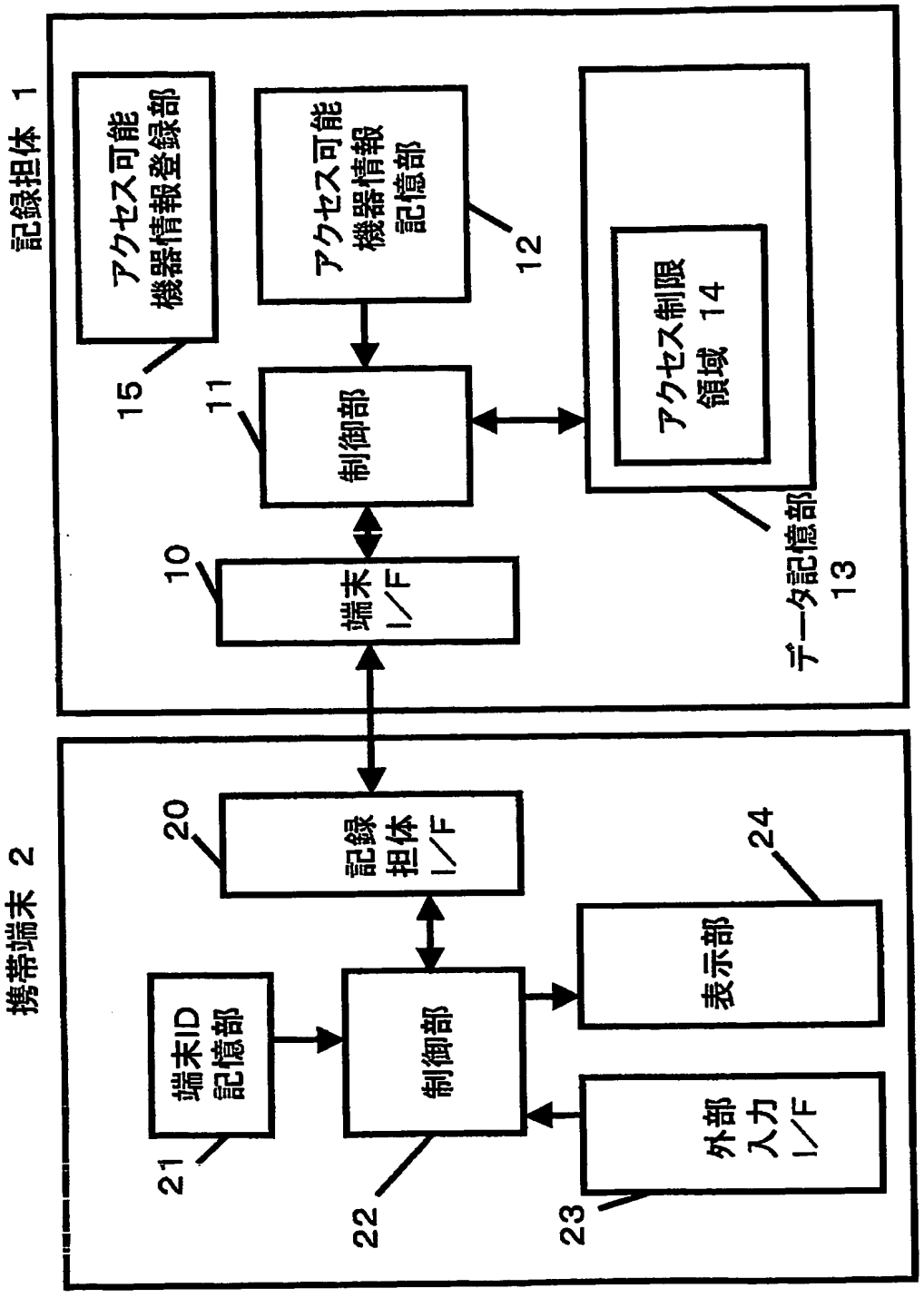
【図６】本発明の実施の形態２に係るアクセス可能機器情報登録時のアクセス可能機器情報配信サーバー７及びユーザー端末８の構成を示すブロック図

【符号の説明】

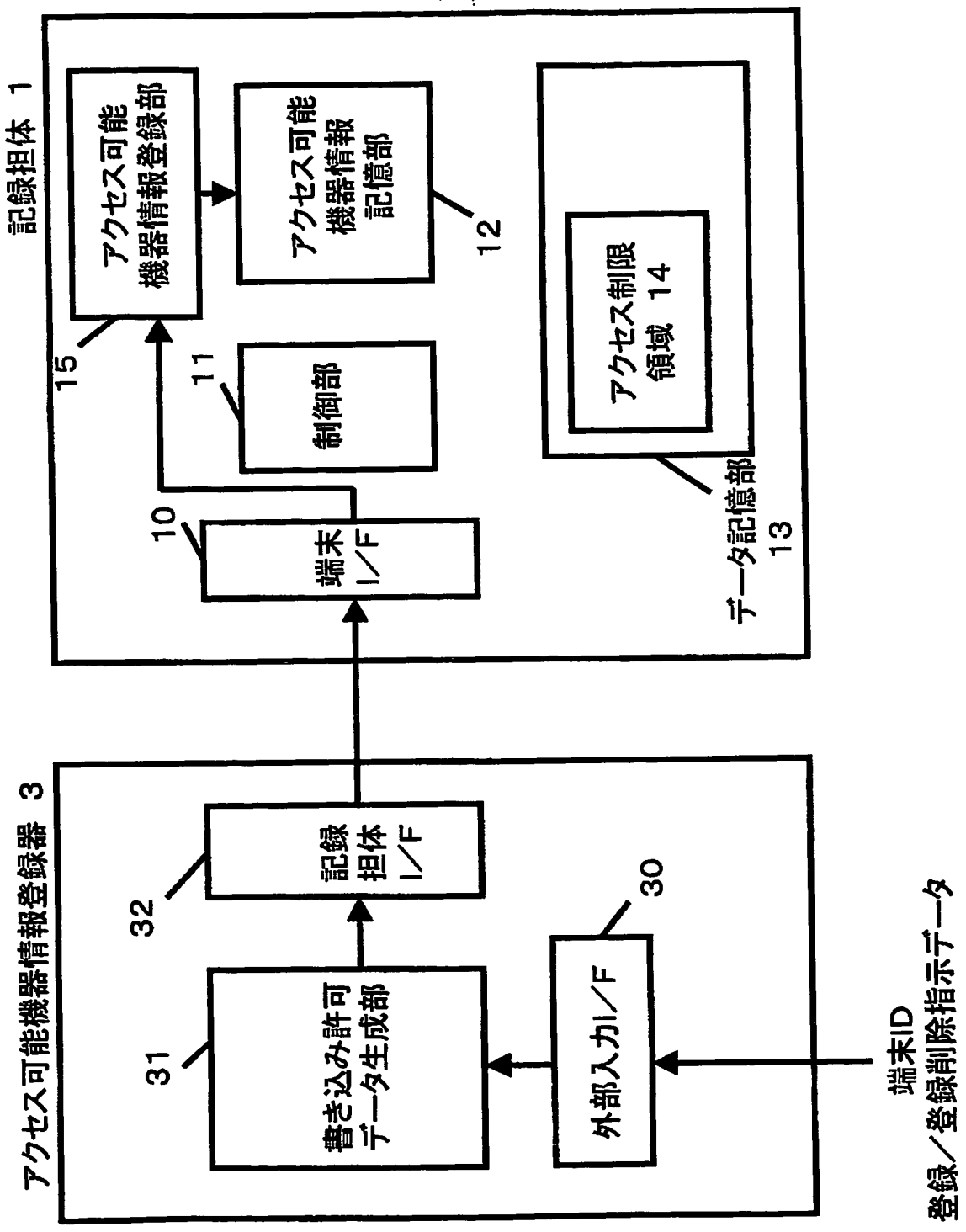
【００６７】

１，５　　記録担体
２，６　　携帯端末
３　　アクセス可能機器情報登録器
４　　アクセス可能機器情報配信サーバー
７　　アクセス可能機器情報管理サーバー
８　　ユーザー端末
１０，５０　　端末Ｉ／Ｆ
１１，２２，５１，６２，８１　　制御部
１２，７０　　アクセス可能機器情報記憶部
１３，５３　　データ記憶部
１４，５４　　アクセス制限領域
１５，７１　　アクセス可能機器情報登録部
１６，５５　　カードＩＤ記憶部
２０，３２，６０　　記録担体Ｉ／Ｆ
２１，６１　　端末ＩＤ記憶部
２３，３０，４０，６３，８０　　外部入力Ｉ／Ｆ
２４，６４　　表示部
２５，６５，８２　　通信Ｉ／Ｆ
３１，４１　　書き込み許可データ生成部
４２　　データ送信部
５２　　アクセス可能機器情報改ざん検査部

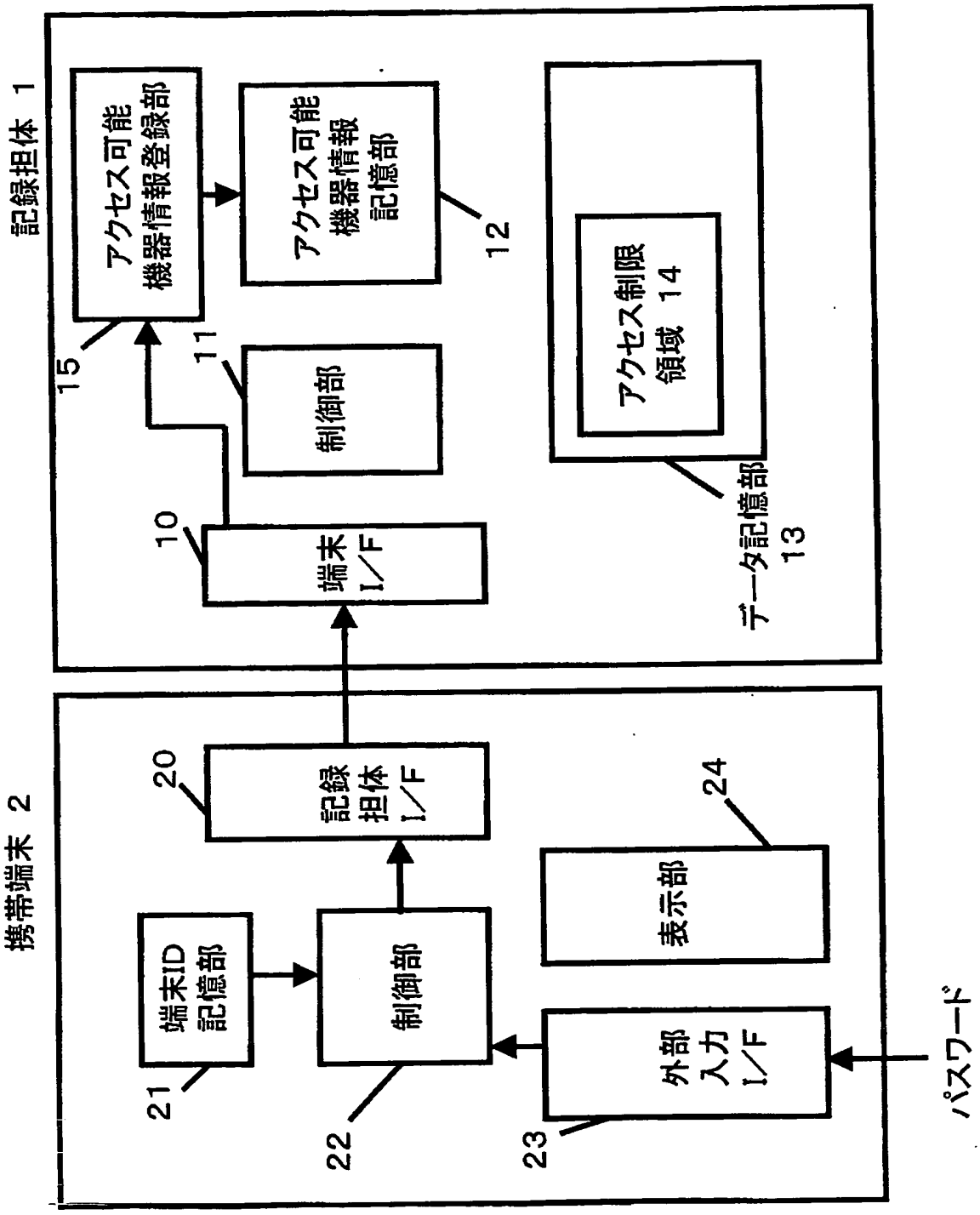
【書類名】図面
【図１】


記録担体 1
アクセス可能機器情報登録部
15
アクセス可能機器情報記憶部
12
制御部
11
端末I／F
10
アクセス制限領域 14
データ記憶部
13
携帯端末 2
記録担体I／F
20
端末ID記憶部
21
制御部
22
表示部
24
外部入力I／F
23

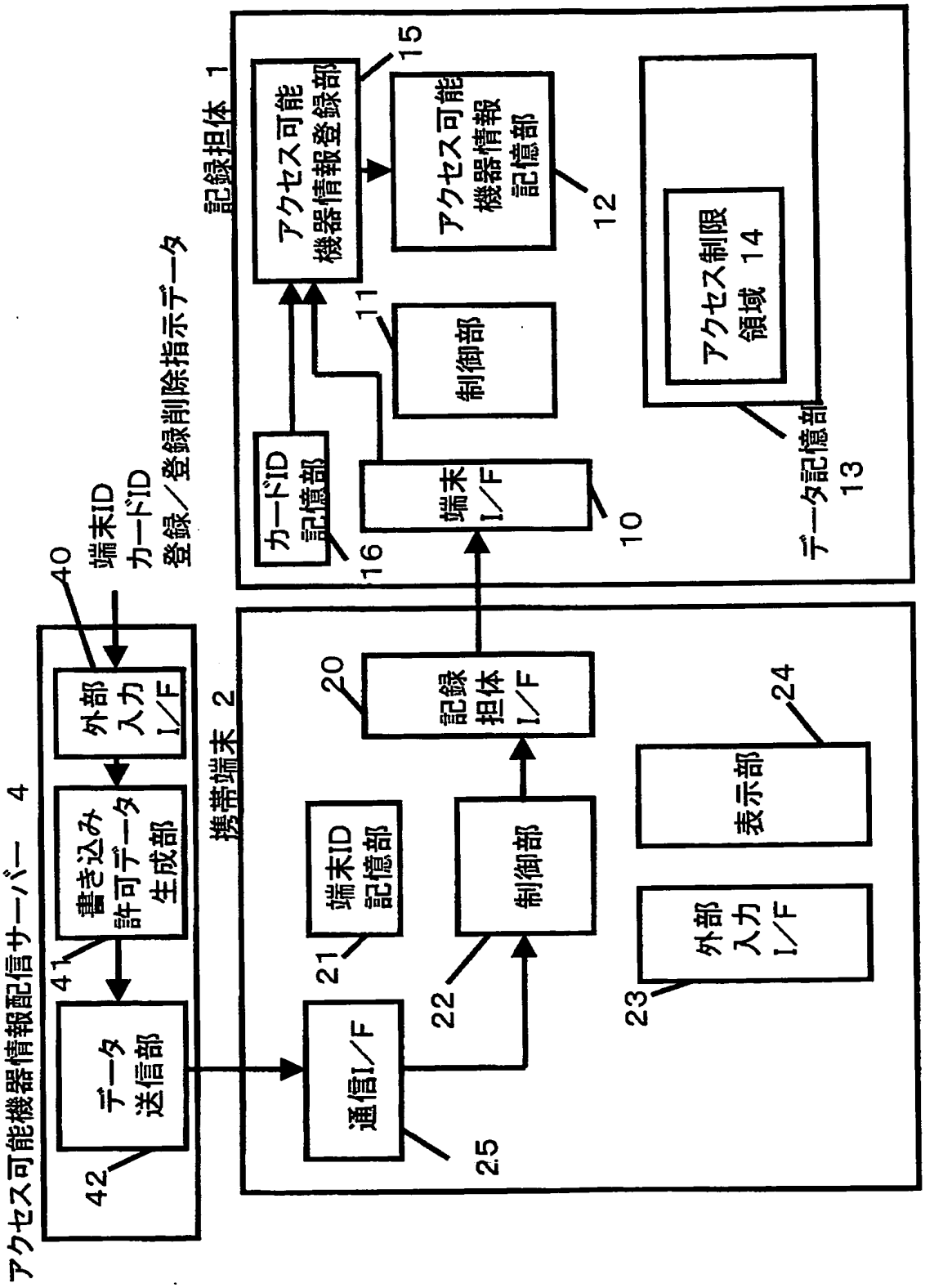
【図２】


記録担体 1
アクセス可能機器情報登録部
15
アクセス可能機器情報記憶部
12
制御部
11
端末I／F
10
アクセス制限領域 14
データ記憶部
13
アクセス可能機器情報登録器 3
書き込み許可データ生成部
31
記録担体I／F
32
外部入力I／F
30
端末ID
登録／登録削除指示データ

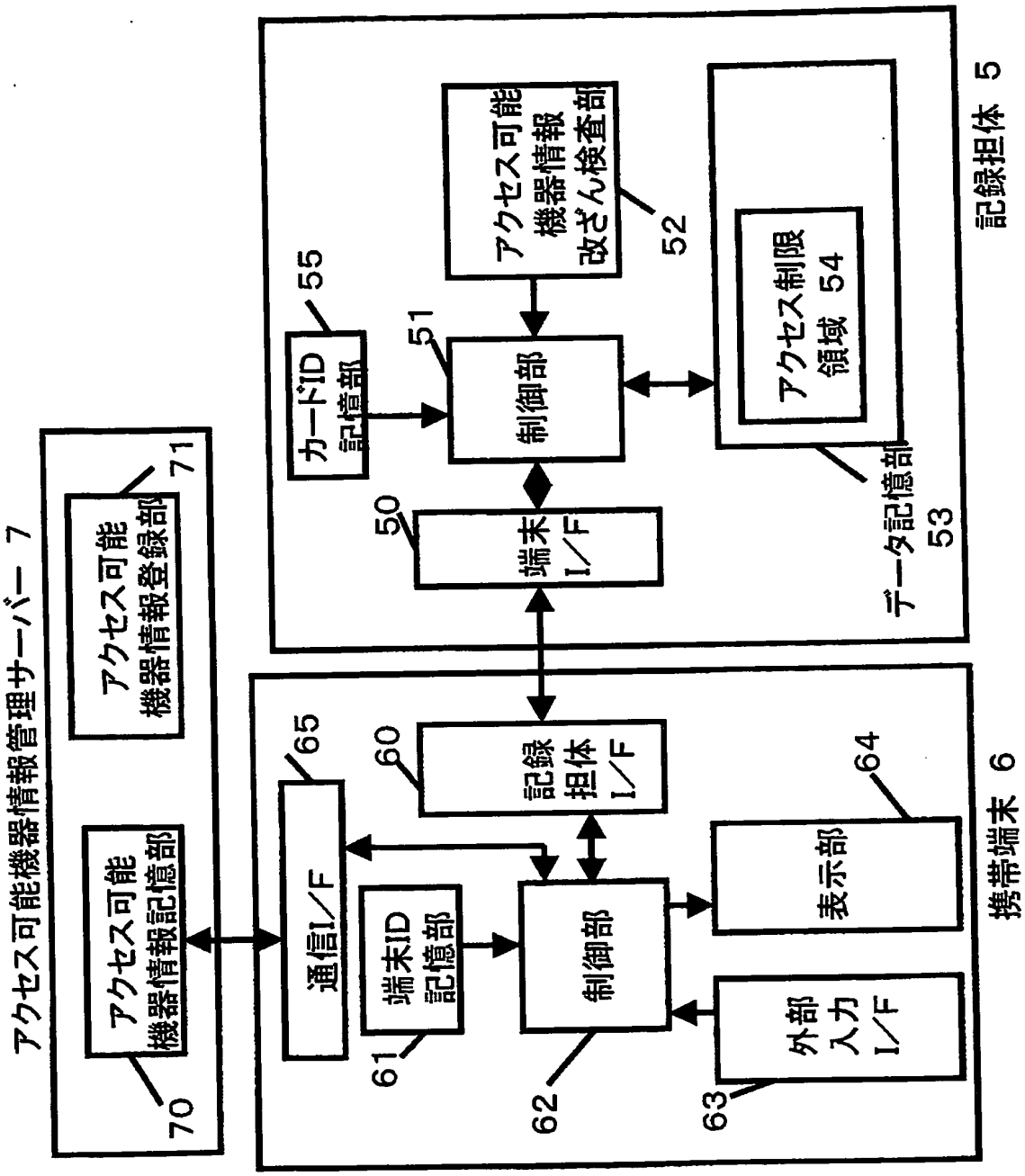
【図３】


記録担体 1
アクセス可能機器情報登録部
15
アクセス可能機器情報記憶部
12
制御部
11
アクセス制限領域 14
データ記憶部
13
端末I／F
10
携帯端末 2
記録担体I／F
20
端末ID記憶部
21
制御部
22
表示部
24
外部入力I／F
23
パスワード

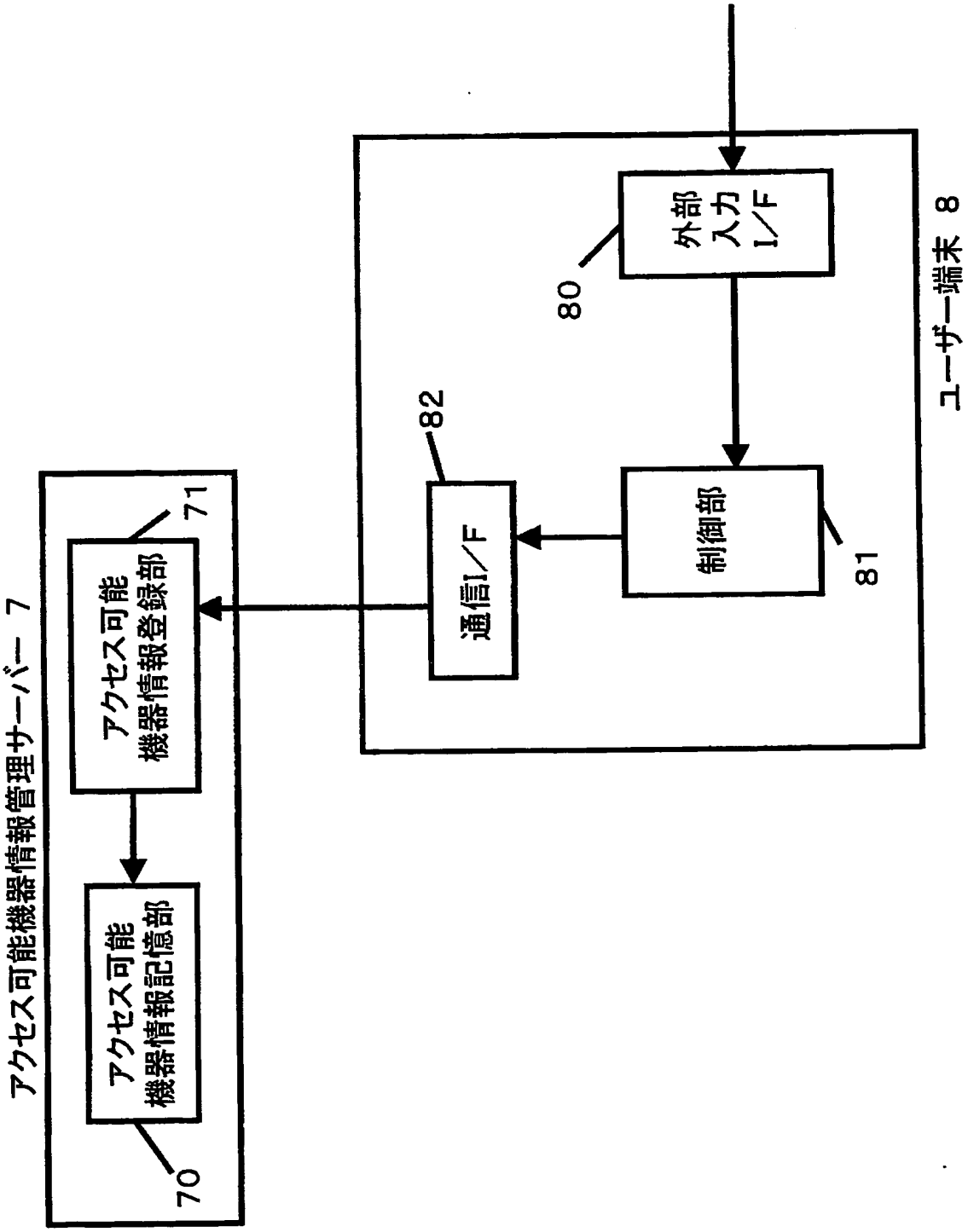
【図４】


アクセス可能機器情報配信サーバー　4
外部入力I／F
40
端末ID
カードID
登録／登録削除指示データ
書き込み許可データ生成部
41
データ送信部
42
携帯端末　2
通信I／F
25
端末ID記憶部
21
制御部
22
記録担体I／F
20
外部入力I／F
23
表示部
24
記録担体　1
カードID記憶部
16
端末I／F
10
制御部
11
アクセス可能機器情報登録部
15
アクセス可能機器情報記憶部
12
アクセス制限領域　14
データ記憶部
13

【図５】


アクセス可能機器情報管理サーバー 7
アクセス可能
機器情報記憶部
70
アクセス可能
機器情報登録部
71
記録担体 5
カードID
記憶部
55
アクセス可能
機器情報
改ざん検査部
52
制御部
51
アクセス制限
領域 54
端末
I／F
50
データ記憶部
53
携帯端末 6
通信I／F
65
記録
担体
I／F
60
端末ID
記憶部
61
制御部
62
表示部
64
外部
入力
I／F
63

【図６】


アクセス可能機器情報管理サーバー 7
アクセス可能
機器情報記憶部
70
アクセス可能
機器情報登録部
71
通信I／F
82
制御部
81
外部
入力
I／F
80
ユーザー端末 8

【書類名】要約書
【要約】
【課題】メモリカード盗難時に、記憶内容の不正読み取りを防止すること。
【解決手段】メモリカード内に、アクセス可能な端末の端末ＩＤリストを格納する手段と、それに基づいて端末からのアクセスの許可／不許可を判断する手段とを備えることによって、アクセス許可されていない端末によるメモリカード読み取りを防止し、正規カード保有者にとって操作の面で大きな負担をかけず、かつ、オフライン環境下でのカード内データの覗き見も防止することができる。
【選択図】図１

特願２００３－３５６０７２

出　願　人　履　歴　情　報

識別番号　［０００００５８２１］

１．変更年月日　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社